UNIVERSITY OF SASKATCHEWAN

Department of Computer Science

CMPT 434.3 FINAL EXAMINATION

December 22nd, 2004

Total Marks: 100

Time: 3 hours

CLOSED BOOK and CLOSED NOTES
NO CALCULATOR

Instructions

Read each question carefully and write your answer legibly on the examination paper. **No other paper will be accepted**. You may use the backs of pages for rough work but all final answers must be in the spaces provided. The marks for each question are as indicated. Allocate your time accordingly.

Ensure that your name AND student number are clearly written on the examination paper and that your name is on every page.

Question	Marks
1 (10 marks)	
2 (12 marks)	
3 (10 marks)	
4 (14 marks)	
5 (15 marks)	
6 (15 marks)	
7 (12 marks)	
8 (12 marks)	
Total	

Name: ____

Student Number: ______________________________

Name:_______________________________________

Student Number:______________________________

1. **General** (*10 marks in total – 1 mark for each part*) Give the technical term that best fits each of the following descriptions or definitions.

(a) Defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.

(b) The field in the UDP segment header that is used by a host to demultiplex (i.e., direct to the appropriate receiving process) an incoming stream of UDP segments.

(c) A protocol providing call setup and management functions in applications such as Internet telephony.

(d) An Internet protocol that allows routers to forward datagrams based on fixed-length labels rather than destination IP addresses, effectively blending virtual circuit techniques into a routed datagram network.

(e) The time required for a bit to travel from one end of a link to the other end.

(f) A protocol widely used in e-commerce applications to provide data encryption and authentication between Web clients and servers.

(g) A specification of how to send email that includes other than ordinary ASCII text, such as images and audio.

(h) A point-to-point link layer protocol widely used in the Internet, such as on dial-up links connecting residential Internet users to their ISP.

(i) A wireless device using 802.11 needs to find and “associate” with one of these to be able to connect to the Internet.

(j) A technique whereby the hosts within a local network can simultaneously share the same “public” IP address for external traffic, while using different “private” IP addresses internally.

2. **Network Architecture** (*12 marks in total*)

(a) (*6 marks*) A basic design principle in the Internet is that of "end-to-end design", in which the objective is to keep the core of the network simple, at the possible cost of requiring extra complexity in the end systems. Briefly describe three examples of the use of this principle in the Internet.

(b) (*6 marks*) Some in the networking community argue that the network core must become more complex, with a richer set of services, if emerging and future application requirements are to be met. What types of applications are of concern here, and why might they need better support from the network core?

3. **Application Layer** (*10 marks in total*)

(a) (*4 marks*) What transport layer protocol does DNS use, and why?

(b) (*6 marks*) One of the most important current applications of the Internet is *content delivery*, in which items such as informational web pages, music files, and videos are delivered to potentially large numbers of geographically dispersed clients. Outline the main techniques that have been devised to make delivery *scalable*; i.e., able to efficiently serve (without overloading servers or network links) large numbers of clients concurrently accessing highly popular items.

4. **Transport Layer** (*14 marks in total*)

(a) (*4 marks*) In addition to increased delays and packet loss, network congestion can result in inefficient use of network resources. Explain.

(b) (*4 marks*) State how the *congestion window* (as measured in maximally-sized segments) is changed in TCP Reno in response to each of the following events:

(i) Packet loss signaled by triple-duplicate ACK.

(ii) Packet loss signaled by timeout.

(iii) An ACK is received for previously unacknowledged data when in the congestion avoidance phase.

(iv) An ACK is received for previously unacknowledged data when in slow-start.

(c) (*6 marks*) Although TCP congestion control has been largely successful at limiting congestion in the Internet, in some contexts it does have some substantial drawbacks. Describe what you feel to be the main disadvantages of the current TCP congestion control algorithm.

Student Number:_______________________________

5. **Network Layer** (*15 marks in total*)

(a) (*6 marks*) List *six* fields in the IPv4 header, briefly stating the purpose of each.

(b) (*6 marks*) Compare the *distance vector* and the *link state* approaches to network routing with respect to the key properties that you feel would impact the choice between them.

(c) (*3 marks*) With IP multicast, how do applications *send* data to multiple receivers, and how do applications *receive* such data?

Student Number:______________________________

6. **Link Layer, Local Area Networks, and Wireless** (*15 marks in total*)

(a) (*6 marks*) Describe how the ALOHA, CSMA, and CSMA/CD protocols differ from each other, and for each protocol give a context in which it would be more suitable than the others.

(b) (*6 marks*) When a frame is received by a link layer switch, how does it know which outgoing interface to send the frame out on? Explain.

(c) (*3 marks*) Supporting mobility between subnets while retaining open TCP connections is harder to do than if the mobile user only moves between LANs within the same subnet. Why?

Student Number:______________________________

7. **Multimedia Networking** (*12 marks in total*)

(a) (*6 marks*) Three basic approaches to dealing with packet loss are *retransmission*, *loss concealment*, and *FEC*. Give the respective advantages/disadvantages of these approaches in the context of multimedia networking.

(b) (*6 marks*) In the current Internet, a streaming video application must adapt its data rate according to both the current network conditions and the capabilities of the client(s). Describe three techniques used in rate control for such applications.

Student Number:______________________________

8. **Security** (*12 marks in total*)

(a) (*3 marks*) MD5, AES, and RSA are all cryptographic algorithms. State the type of each.

(b) (*3 marks*) In public key cryptography, what is a *certificate*, and how is it used?

(c) (*6 marks*) Use of symmetric key cryptography requires that the communicating parties establish a shared secret key. Describe two ways in which this can be accomplished when the parties are geographically separated; i.e., over a network.

The End